EXHIBIT 20

BITCOIN MAGAZINE®

TARI INTRODUCES A BLOCKCHAIN PROTOCOL FOR DIGITAL ASSETS BUILT ON MONERO

Tari protocol enables consumers and business to sell and trade scarce digital assets with programmed rules, and record immutable transfer and verification of ownership.

ERIK KUEBLER • MAY 22, 2018

Tari, a new open-source blockchain protocol, aims to redefine the digital asset experience. Backed by institutional investors including Redpoint, Trinity Ventures, Canaan Partners, Pantera and Multicoin Capital, its founders Riccardo "fluffypony" Spagni, lead maintainer of the Monero cryptocurrency; Naveen Jain, a serial entertainment industry entrepreneur; and Dan Teree, co-founder of Ticketfly, hope to simplify the management, trade, programmability and use of all digital assets.

CURRENT STATE OF DIGITAL ASSETS

"Today, most digital assets such as event tickets, in-game items, loyalty points and virtual currencies are siloed due to restrictions that limit their use and secondary market trade," Jain said in an interview with *Bitcoin Magazine*.

Businesses primarily enact these restrictions to control assets after their distribution, verify an asset holder's identity and prevent fraudulent counterfeiting.

Siloed digital assets aren't ideal for consumers or businesses. Consumers don't enjoy "true" ownership of the digital assets they purchase or earn because they must comply with secondary market restrictions and regulations, and businesses miss out on billions of dollars generated from the secondary digital asset resales that occur on outside channels.

For example, consider a frequent Delta flyer who takes one Lufthansa flight a year and is unable to trade his or her Lufthansa miles (that are unlikely to be redeemed) for Delta miles. Or, the millions of dollars in ticket resale revenues that artists like Beyoncé miss out on after issuing tickets for their world tours. Once Beyoncé sells a $100 ticket to the

original buyer, she does not participate in the secondary market resale economics when the original buyer resells his or her ticket for $500, and the secondary market scalper turns around and sells the ticket a third time for $1000 the night before the show.

REVAMPED DIGITAL ASSETS

By leveraging blockchain technology, the Tari protocol enables consumers and business to break down walled gardens between businesses, sell and trade scarce digital assets with programmed rules, and record immutable transfer and verification of ownership.

The Tari protocol hopes to unlock additional utility for digital asset users and enable "true" digital asset ownership and control. By utilizing the Tari protocol, the aforementioned Delta flyer can perhaps trade his or her Lufthansa miles for Delta miles. And artists like Beyoncé can issue their world tour tickets with programmed rules that allow them to capture and control secondary market value. Beyoncé could hard-code rules such as: tickets can only be resold three times, Beyoncé is entitled to 10 percent of any ticket resale, and tickets are not re-sellable 24 hours before the show.

John Pleasants, former CEO of Ticketmaster and COO of Electronic Arts, thinks that the Tari protocol will open up free trade between a variety of industries."[Tari] can help the entire live entertainment industry recover billions in lost revenue by better controlling how tickets are sold and resold. From a gaming perspective, the ability to buy and sell virtual goods on a distributed system across different platforms can greatly improve both monetization for publishers and the overall consumer experience."

TARI PROTOCOL: UNDER THE HOOD

According to Spagni, the Tari protocol will be built on top of Monero. Specifically, Tari will be a merged-mined sidechain of Monero. Merged-mining allows for two cryptocurrencies to be mined simultaneously based on the same algorithm. In this case, it is Monero's proof of work algorithm that miners must solve.

The Tari token powers the Tari protocol, serves as an incentive for miners to mine Monero and for valiators to accurately validate the network's rules.

"To give miners an incentive to merged-mine your chain, there needs to be a reward. We can't pay them in Monero, so we need to have a native token that merged-miners receive. Tari tokens will also be used as an incentive for rule validation. Users have the opportunity to put Tari tokens in an escrow account and passively run a program that validates [protocol] rules on their computer. If they behave and validate the rules correctly, they will earn tokens and keep their escrow," explained Spagni.

MERGED-MINING WITH MONERO

Because Tari is merged-mining, the team doesn't have to recruit new miners. Instead, Monero mining pools can "flip a switch" (tweak their settings) and mine both Monero and Tari simultaneously. Spagni also pointed out that merged-mining with Monero's proof of work system doesn't incur additional electricity costs or environmental damage risks traditionally associated with proof of work, since miners aren't burning more cycles.

Spagni also noted that, “All the proof of work chains burn less electricity than Visa. We are getting to a point where a solid proof of work chain can provide the same, if not greater, capabilities of Visa.”

TARI COMMUNITY

The Tari team noted that there is no “core team” for Monero. Jain noted, “We don’t want single points of failure. We are co-founders and contributors. But, not the only contributors. There are lots of smart people within and outside the organization. We want far more external contributors than internal contributors. In fact, we want hundreds if not thousands of contributors over time.”

For reference, the Monero protocol had around 150 contributors within the last 12 months.

POTENTIAL ISSUES

Although Tari aims to revamp the way consumers and businesses interact with digital assets, the team has various obstacles to overcome.

ADOPTION

Is it favorable for businesses to allow their assets to trade on a secondary market? And will businesses amend their terms and user agreements to allow secondary market liquidity for their digital assets? For example, airline loyalty points are currently an illiquid market. Wall Street analysts have pointed out that the sale of these loyalty points can equal up to half of an airline’s yearly earnings before interest and taxes, but airlines might want loyalty points to expire unredeemed. That way, airlines can increase revenue, without having to discount travel for customers who don’t take advantage of their loyalty points.

SCALABILITY

Because the Tari protocol intends to become the underlying protocol for the transfer of digital assets, they will need to handle “many tens of thousands of transactions per second,” according to Jain. The team plans to use lightning as the primary throughput mechanic for Tari.

Spagni explained, “We’re building a standards compliant lightning router, that will be compatible with Bitcoin, Monero and Tari. We will also achieve additional throughput by building a MimbleWimble chain. This way, transactions won’t be stored on the blockchain in their entirety, just kernels.”

The Tari protocol has yet to deploy a test network boasting any transaction capabilities, not to mention Visa-level performance.

Disclosure: The author has an investment in Tari.

BITCOIN MAGAZINE®

FEATURE

HOW TARO BRINGS ASSETS TO BITCOIN THROUGH TAPROOT AND LIGHTNING

Taro, a new protocol proposed by Lightning Labs, leverages Taproot and the Lightning Network to bring new assets and scalability to Bitcoin.

NAMCIOS • APR 5, 2022

Lightning Labs has introduced a new protocol proposal for Bitcoin and the Lightning Network, Taro, which seeks to bring new use cases to the network. The company has published a series of draft Bitcoin Improvement Proposals (BIPs) and it is asking for community feedback on the proposed design.

Taro seeks to enable the issuance of assets and collectibles, which are the protocol's form of non-fungible assets, on Bitcoin as well as their transfer on Lightning in a private and secure manner without bloating the blockchain. To do so, it plans to leverage the protocol's latest upgrade, Taproot.

"The design principles of Taro on Lightning draw from that of the internet, where you have complexity at the edges, but you keep the simplicity in between," Elizabeth Stark, Lightning Labs CEO, told *Bitcoin Magazine*.

Most existing ways to issue and use assets on Bitcoin today either leverage another blockchain entirely, which adds a new trust model with different security assurances, or rely on adding extra

data directly on-chain, which is inefficient for keeping track of asset information long term and is dangerous to user privacy.

Instead, Taro uses Taproot.

THE FUTURE OF TAPROOT: SCALABILITY AND PRIVACY

Taproot allows complex spending conditions to be set for a Bitcoin UTXO while ensuring that only the condition that ultimately gets used to spend the coin is revealed on-chain to all Bitcoin users. As a result, such a spend is more private, because a passive observer can't tell if there were other spending conditions for that transaction; and more scalable, because now that complex scheme puts considerably less data on chain. This is meaningful because previous programmatic behaviors in Bitcoin meant transactions had to be revealed in their entirety whenever they were spent, hurting user privacy and making very complex schemes unfeasible due to a linear growth in storage needs.

By using Taproot, Taro can also rely on Bitcoin's proof-of-work (PoW) consensus mechanism for ensuring the correct ordering of transactions and preventing double spends, while defining special directives as to how to interact with and validate the new asset data.

As a result, Taro also differs from other asset solutions on "highly programmable" blockchains, such as Ethereum's ERC-20 and ERC-721 tokens, because it is based on Bitcoin's UTXO model instead of an account model, meaning that it is both more secure due to avoidance of key reuse and more private as there isn't information about balances revealed. Taro's approach is also more scalable and is compatible with light clients.

More specifically, Taro brings assets to Bitcoin through the "leaves" of the Taproot script tree, as each leaf in the tree is completely independent and can be selectively revealed — which enables structured commitment. By adding information about those assets (known as metadata) in the Taproot script tree, the proposed protocol can function as a layer built on top of Bitcoin, allowing Taro asset transactions to look like regular Bitcoin transactions, as on-chain only the Taproot output is revealed, while still enabling proofs of the movement of assets across the transaction graph.

BITCOIN IS SCALABLE

"This is pretty elegant because it lets you separate these asset commitments from the actual script itself," Lightning Labs CTO, Olaoluwa Osuntokun, told *Bitcoin Magazine*. "Taproot, in this case, allows us to logically separate what is the main Bitcoin scripting layer from the asset layer itself. Even though they're actually within the same output, because the Bitcoin layer doesn't care about what isn't revealed, we can use that to have additional structured data."

As a result, this construction enables a single Taproot UTXO to effectively commit to (that is, include the hash of) an unbounded number of assets that are only revealed to the specific parties that need that information — without burdening the entire Bitcoin network.

"It makes things a little bit simpler and also makes it a lot easier for developers to understand because the overlay layer basically looks and feels like Bitcoin with some slight tweaks, additional commitments, validation, things like that," Osuntokun said.

By leveraging Taproot for asset issuance and transfer, Taro effectively enables new functionality at the edges of Bitcoin by leveraging bitcoin liquidity as the asset gets routed through the Lightning Network, all without adding unnecessary data on chain.

"If people are doing more transactions at the edges using these assets, well, that means we actually need more capacity in the Lightning Network itself," Osuntokun said. "Demand for assets at the edges, as far as structural capacity, then translate into increased productive activity on the network and more routing fees, so a greater network effect as well."

As a result, Taro can take one step in the direction of increasing the demand for blockspace on chain, helping ensure that Bitcoin can keep sustainable once miners begin being paid only through transaction fees as the block subsidy nears zero in the next century.

A TWEAKED MERKLE TREE

Taro leverages a data structure known as a Merkle-Sum Sparse Merkle tree (MS-SMT) to enable assets to commit to Taproot script trees, acting as an overlay protocol. MS-SMT joins together properties of a regular Merkle tree, a Merkle-Sum tree, and a Sparse Merkle tree.

A Merkle tree is constructed by hashing a list of items' hashes in pairs until we arrive at a single hash, called the root hash. For example, in a list of four items, we would first separately hash each item. Next, we would join the hashes of items one and two together and hash that concatenation, and do the same with the hashes of three and four. Lastly, we would hash the remaining two hashes to determine the root hash.

A Merkle tree is useful because it can store lots of data, it makes it easy to prove that some data exists in the tree, and it also allows us to check that data hasn't been tampered with. In other words, a regular Merkle tree enables scalability, proof of membership and tamper resistance.

Moreover, we only need to store the root hash of the Merkle tree on chain to verify such properties. That's because if the data in one leaf is tampered with, for example, its hash would also change, further changing all of the hashes at levels above it which would lastly change the root hash — which can have its change attested through comparison to the stored version.

The Merkle-Sum tree takes this one step further by allowing us to commit to the sum of all leaf values, meaning its root hash can also include information about the sum of the values of each leaf in the tree. In the context of assets, this property enables an asset's supply to be more easily audited, as well as allowing the divisibility of the asset and preventing undesired issuance of new assets in transactions that are only supposed to transfer them. In our fictitious Merkle tree above, if each leaf held a value of one, the root hash would hold a value of four.

The Sparse Merkle tree adds yet another property. All of its leaves are indexed, allowing access to information on the tree in a key-value pair fashion, and it has empty leaves, which actually hold the "null" value, allowing us to check if some data is *not* in the tree. This property, known as proof of non-membership, is possible by *proving membership of null* in a given leaf which can be accessed through its index. For example, if there is a claim that the leaf with index six stores some information about an asset, we can prove that such information is not there by attesting that that leaf actually holds a value "null."

TRANSFERRING A TARO ASSET

Taro represents assets with nested MS-SMTs, one for each asset ID or asset type. The protocol enables those trees to be layered on top of each other, branching out of the initial Taproot script tree to represent an effectively unlimited number of assets in a single Taproot UTXO. Taro assets are therefore issued on chain.

At the basis of asset functionality on Taro is an asset script, a set of directives established by a developer to programmatically define how a given asset can be transferred on the protocol. The hash of that script is then included in the MS-SMT so it can be easily enforced later on — thereby making the asset and its attributes commit to the asset script hash.

The initial version of Taro proposes the use of a subset of Bitcoin Script, allowing assets to express arbitrary conditions for the valid transfer of an asset. As asset scripts inherit a level of programmability on par with Bitcoin Script, Taro assets can be transferred over Lightning in multi-hop transactions off-chain through hash time locked contracts (HTLCs) embedded in the asset script. However, future versions could introduce new opcodes and extra functionality that would only exist at the Taro level.

"Doing Taproot-within-Taproot makes the initial version simpler and gives us more time to figure out what use cases pop up and desire more expressivity," Osuntokun said.

For on-chain transfers, Taro leverages a new address format based on bech32 that also includes the asset script hash. To receive a Taro asset on chain, the receiver would need to create an address with enough data that details how the sender can construct a new asset script group that contains the information needed to spend the asset once it is transferred over to the new owner. In other words, the extra information, in the asset script hash, tells the receiver what the unlocking capability is for the asset that is being transferred, so that it can eventually be transferred again.

Since the receiver has all of that information, they can compute the asset leaf, which then lets them compute the asset root, and finally the entire output itself, letting them watch the Bitcoin blockchain for the result they computed.

Additionally, by having the receiver send that defining information beforehand, the only way the sender can make the transaction valid is if they send exactly what the receiver is expecting. If the wrong asset or the wrong amount is sent, the hashes won't match and the receiver can easily tell that the sender did something wrong.

ASSETS AND COLLECTIBLES ON BITCOIN

The issuance and transfer of assets in Taro vary, depending on whether the asset is a regular one or a collectible.

A collectible, or non-fungible asset, is a one-of-a-kind representation of value, with a unique identifier that establishes a claim on an asset at the Bitcoin chain level or at the real-world level and makes it impossible to counterfeit ownership. A collectible on Taro could be a tokenized rare baseball card, for example. Collectibles are created in a single batch transaction, cannot be split or merged, and need to be transferred off-chain or put into a multiparty channel to be transferred among a known set of participants.

A regular asset, on the other hand, commits to a total value of held assets and can be split and merged. Splits can happen within a tree, configuring an internal split, or across different Taproot outputs, configuring an external split. During transfer, the asset holder proves they hold a valid split with a Merkle-Sum proof and the corresponding created assets commit to a new Merkle-Sum output split that ensures the total amount of assets after transfer equals the total amount there was before the transaction.

ASSETS AT THE EDGES: LIGHTNING AS A DECENTRALIZED BACKBONE PAYMENT NETWORK

As mentioned earlier, Taro can port assets issued on-chain onto the Lightning Network, similar to how bitcoin can be sent through Lightning after being locked up in a two-of-two multisignature output that gets confirmed on the Bitcoin blockchain. A Lightning channel holding Taro assets leverages the same flow, however the two-of-two Schnorr Taproot output would also commit to the set of assets in the channel.

“Using the Taro protocol, Lightning channels anchored with a Taproot output are able to send both bitcoin and Taro assets off-chain, with multi-hop payments being facilitated by new HTLCs on the Taro level, which use the scripting system to implement the expected end-to-end payment security guarantees,” Osuntokun told *Bitcoin Magazine*.

Osuntokun added that Lightning Labs’ proposed deployment path for Taro on the Lightning Network seeks to first only introduce assets at the edges, meaning it would avoid both having to modify the core of the network and bootstrap a new network with adequate liquidity for each Taro asset. Rather, the company’s plans would have Taro plug into bitcoin liquidity on Lightning and require only the sender and receiver of a given asset to use Taro-aware channels.

“The only constraint is that in order to receive/send using a particular asset, corresponding inbound/outbound liquidity is required,” Osuntokun said.

In addition to the similar Lightning on-ramp setup, multi-hop transfers of Taro assets over Lightning would leverage a similar invoicing system that is commonplace on the second layer today. However, instead of denominating the invoice in BTC, the invoice would be denominated in the Taro asset itself.

"As an example, if Alice wants to send Bob a Taro stablecoin asset, she'll create a new invoice that quotes, say, $10," Osuntokun said. "Bob will then use a 'hop hint,' which are extra routing details provided in the invoice to complete the route and calculate the amount of network fees (paid in bitcoin) to send over his first hop, which will traverse the internal Bitcoin backbone and eventually drop off enough BTC at the final hop to complete the payment."

The Taro protocol will specify the extra information that needs to be sent to the Lightning peers at the edges in order to update all channels properly, he added.

MAKING BITCOIN THE DE-FACTO BASE LAYER

Taro seeks to leverage Bitcoin's latest soft fork upgrade to bring assets with real-word use cases like U.S. dollar stablecoins onto the peer-to-peer (P2P) digital currency stack. It enables the issuance of a nearly unlimited number of assets with a single Taproot UTXO, as well as the transfer of such assets with instant, low-fee multi-hop transactions on Lightning.

By leveraging Bitcoin and Lightning as its rails, Taro could establish an interoperable ecosystem of assets that can unite different use cases while not affecting parties that may not care about such assets. At the same time, the protocol also contributes back to Bitcoin by increasing its network effects in the event that a popularization of the concept drives traffic on the network, thereby increasing the fee payout to miners and ramping up BTC liquidity on the Lightning Network.

Though its initial iteration accommodates a limited number of use cases, in an attempt to make the jump onto the new protocol easier for developers through a familiar Bitcoin scripting suite, the possibilities of extensions and further developments are nearly endless, as builders and entrepreneurs get creative and spin the protocol to suit their needs.

"The hope is to open up people's eyes to what the future of Bitcoin holds and what Taproot can enable," Stark told *Bitcoin Magazine*. "The goal is to have Bitcoin be the underlying global monetary network powered by open protocols."